

News & Analysis

Toyota Case: Single Bit Flip That Killed

Junko Yoshida

10/25/2013 03:35 PM EDT

[107 comments](#)

Tweet

Share

G+

MADISON, Wis. — Could bad code kill a person? It could, and it apparently did.

The Bookout v Toyota Motor Corp. case, which blamed sudden acceleration in a Toyota Camry for a wrongful death, touches the issue directly.

This case -- one of several hundred contending that Toyota's vehicles inadvertently accelerated -- was the first in which a jury heard the plaintiffs' attorneys supporting their argument with extensive testimony from embedded systems experts. That testimony focused on Toyota's electronic throttle control system -- specifically, its source code.

The plaintiffs' attorneys closed their argument by saying that the electronics throttle control system caused the sudden acceleration of a 2005 Camry in a September 2007 accident that killed one woman and seriously injured another on an Oklahoma highway off-ramp. It wasn't loose floor mats, a sticky pedal, or driver error.

An Oklahoma judge announced that a [settlement to avoid punitive damages](#) had been reached Thursday evening. This was announced shortly after an Oklahoma County jury found Toyota liable for the crash and awarded \$1.5 million of compensation to Jean Bookout, the driver, who was injured in the crash, and \$1.5 million to the family of Barbara Schwarz, who died.

During the trial, embedded systems experts who reviewed Toyota's electronic throttle source code testified that they found Toyota's source code defective, and that it contains bugs -- including bugs that can cause unintended acceleration.

"We've demonstrated how as little as a single bit flip can cause the driver to lose control of the engine speed in real cars due to software malfunction that is not reliably detected by any fail-safe," Michael Barr, CTO and co-founder of Barr Group, told us in an exclusive interview. Barr served as an expert witness in this case.

A core group of seven experts, including four from Barr Group, analyzed the Toyota case. Their analysis ultimately resulted in Barr's 800-plus-page report.

In Toyota's own view, though, the automaker had been already exonerated when the National Highway Traffic Safety Administration closed its probe of Toyota models in February 2011. The NHTSA decision came after NASA investigated Toyota's electronic throttle control system and found no electronic causes of unintended acceleration during a 10-month review.

But not everyone in the embedded systems industry thinks NASA had enough time to come up with a complete report. Perhaps more significantly, in its report, [NASA itself did not rule](#)

out the possibility of software having caused unintended acceleration.

The group of seven experts was given the task of picking up where the NASA investigation left off.

"We did a few things that NASA apparently did not have time to do," Barr said. For one thing, by looking within the real-time operating system, the experts identified "unprotected critical variables." They obtained and reviewed the source code for the "sub-CPU," and they "uncovered gaps and defects in the throttle fail safes."

Further, the team ran simulations in the Green Hills Simulator. "This confirmed tasks can die without the watchdog resetting the processor." His group also independently checked worst-case stack depth. "We found many big mistakes in the Toyota analysis that NASA relied on."

The experts demonstrated that "the defects we found were linked to unintended acceleration through vehicle testing," Barr said. "We also obtained and reviewed the source code for the black box and found that it can record false information about the driver's actions in the final seconds before a crash."

It's important to note Barr Group testimony led to a [billion-dollar economic-loss settlement](#) by Toyota last December. Because of that settlement, details of the technical discoveries made back then by the experts were not made public until the Oklahoma trial. The economic-loss settlement resolved hundreds of lawsuits claiming vehicles depreciated after the company issued recalls related to faulty acceleration. Toyota still faces lawsuits claiming injury or death related to the recalls.

Task X death

Now that the experts' testimony and findings have been made public through the Oklahoma trial, let's get into details. What defects were found in Toyota's electronic throttle control systems?

Barr said that the 2005 Camry L4 source code and in-vehicle tests by the experts confirmed that some critical variables are not protected from corruption, and sources of memory corruption are present. He believes that Toyota's engineers sought to protect numerous variables against software- and hardware-cause corruptions, but they failed to mirror several key critical variables, and they made no hardware protection available against bit flips.

Stack overflow and software bugs led to memory corruption, he said. And it turns out that the crux of the issue was these memory corruptions, which acted "like ricocheting bullets."

Barr explains the issue this way:

Memory corruption as little as one bit flip can cause a task to die. This can happen by hardware single-event upsets -- i.e., bit flip -- or via one of the many software bugs, such as buffer overflows and race conditions, we identified in the code. There are tens of millions of combinations of untested task death, any of which could happen in any possible vehicle/software state. Too many to test them all. But vehicle tests we have done in 2005 and 2008 Camrys show that even just the death of Task X by itself can cause loss of throttle control by the driver -- even as combustion continues to power the engine. In a nutshell, the fail safes Toyota did install have gaps in them and are inadequate to detect all of the ways UA can occur via software.

Just to clarify, the "tasks" are equivalent to apps running on smartphones or PCs. All software malfunctions from time to time -- we often have to reboot our machines. The 2005 Camry L4 has a set of dozens of apps (or tasks). Because they are all meant to be running always, the death of one could have dire consequences.

When asked if the whole case for unintended acceleration could be pinned on the task X death, Barr replied, "The task X death in combination with other task deaths." There are dozens of tasks and 16 million different ways those tasks can die. The experts group was able to demonstrate at least one way for the software to cause unintended acceleration, but there are so many other ways that could have happened.

Barr also said more than half the dozens of tasks' deaths studied by the experts in their experiments "were not detected by any fail safe."

What's next for NHTSA

After the Oklahoma trial, what steps should the NHTSA be taking? Barr made some suggestions:

NHTSA needs to get Toyota to make its existing cars safe and also needs to step up on software regulation and oversight. For example, FAA and FDA both have guidelines for safety-critical software design (e.g., DO-178) within the systems they oversee. NHTSA has nothing.

Also, NHTSA recently mandated the presence and certain features of black boxes in all US cars, but that rule does not go far enough. We observed that Toyota's black box can malfunction during unintended acceleration specifically, and this will cause the black box to falsely report no braking. NHTSA's rules need to address this, e.g., by being more specific about where and how the black box gets its data, so that it does not have a common failure point with the engine computer.

— Junko Yoshida, Chief International Correspondent, [EE Times](#) 

Related posts:

- [Timeline: Toyota Faces More Battles in Liability War](#)
- [Toyota Case: Vehicle Testing Confirms Fatal Flaws](#)
- [Toyota Case: Inside Camry's Electronic Control Module](#)
- [Toyota Trial: Transcript Reveals 'Task X' Clues](#)
- [Why Toyota's Oklahoma Case Is Different](#)
- [Toyota's Killer Firmware: Bad Design & Its Consequences](#)
- [Toyota Case: Single Bit Flip That Killed](#)
- [Acceleration Case: Jury Finds Toyota Liable](#)
- [Oklahoma Jury to Deliberate Toyota Acceleration Case](#)

[EMAIL THIS](#) [PRINT](#) [COMMENT](#)

More Related Links

[Coming Soon \(2018\): The \\$200k Robo-Taxi](#)

[Slow EV Rise Won't Deter NXP's GreenBox](#)

[Venturi Racing Talks Latest Formula E Power Technology](#)

[Nvidia Partners with Continental on Robocars](#)

[Renesas SoC to Double EyeQ5 Efficiency](#)

Copyright © 2018 UBM Electronics, A AspenCore company, All rights reserved. [Privacy Policy](#) | [Terms of Service](#)